UNITED STATES DISTRICT COURT
DISTRICT OF MASSACHUSETTS

ALEYDA TORRES, on behalf of herself and all others similarly situated,
Plaintiff

v.

BAYSTATE HEALTH, INC.,
Defendant

CASE NO.:

CLASS ACTION

COMPLAINT FOR DAMAGES, EQUITABLE, DECLARATORYAND INJUNCTIVE RELIEF
DEMAND FOR JURY TRIAL

Plaintiff Aleyda Torres ("Plaintiff"), individually by and through her undersigned counsel, brings this class action lawsuit against Baystate Health, Inc. ("BHI"), on behalf of herself and all other similarly situated, and alleges, based upon information and belief and the investigation of her counsel, as follows:

INTRODUCTION

1. This is a punitive class action lawsuit brought by current and former patients of BHI against BHI for its failure to properly secure and safeguard their personally identifiable information ("PII") and protected health information ("PHI"), and for their failure to provide timely, accurate and adequate notice that such PII had been compromised.

2. On April 8, 2019, BHI announced that hacker gained access to a number of employee email accounts through a phishing attack which subsequently exposed the personal data of more than 12,000 BHI patients. The exposed personal information included patients' names, dates of birth, addresses, health information (such as, diagnoses, treatment information,

and medications), health insurance information, Medicare numbers and Social Security numbers. ("Data Breach" or "Breach").

3. According to the Notice to Our Patients of an Email Incident ("Notice") issued by BHI, an unauthorized third party illegally accessed a number of BHI employee email accounts.[1] This led to the exposure of personally identifiable information belonging to more than 12,000 BHI patients.

4. While the Breach was discovered by BHI on February 7, 2019, patients were not notified until nearly two months later.

5. Phishing attacks – the kind that led to the Data Breach – are well-known phenomenon for which there are a number of protective measures. This Data Breach occurred, however, only because BHI failed to implement adequate and reasonable cyber-security procedures and protocols. Among other things, Defendant failed to exercise reasonable care, and to implement adequate cyber-security training, including, but not limited to, how to spot phishing emails from unauthorized senders.

6. The deficiencies in Defendant's data security protocols were so significant that the Breach likely remained undetected for months.

7. Intruders, therefore, had months to access, view and steal patient data unabated. During this time, BHI failed to recognize its systems had been breached and that intruders were stealing data on hundreds of thousands of current and former patients. Timely action by BHI would likely have significantly reduced the consequences of the Breach.

8. BHI disregarded the rights of Plaintiff and Class members by intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its

[1] https://www.baystatehealth.org/phishing (last visited on April 10, 2019)

data systems were protected, failing to disclose to its patients the material fact that it did not have adequate computer systems and security practices to safeguard their PII, failing to take available steps to prevent the Data Breach, failing to monitor and timely detect the Data Breach, and failing to provide Plaintiff and Class members prompt and accurate notice of the Data Breach.

9. Plaintiff and Class Members seek to remedy the harms suffered as a result of the Data Breach and have a significant interest in ensuring that their PII, which remain in BHI's possession, is protected from further breaches.

10. No one can know what else the cyber criminals will do with the compromised PII/PHI. However, what is known is that BHI patients will be for the rest of their lives at a heightened risk of further identity theft and fraud.

11. Defendant's conduct gives rise to claims for breach of contract and negligence. Plaintiff, individually, and on behalf of those similarly situated, seeks to recover damages, equitable relief, injunctive relief designed to prevent a reoccurrence of the Data Breach and resulting injuries, restitution, disgorgement, reasonable costs and attorney fees, and all other remedies this Court deems proper.

PARTIES

12. Plaintiff Aleyda Torres is a resident of Springfield, Hampden County, Massachusetts and a patient of BHI. On or about April 5, 2019, Ms. Torres received notice from BHI that her PII/PHI, along with approximately 12,000 patients, had been improperly exposed to unauthorized third parties.

13. Shorty after receiving notice from BHI Health, Ms. Torres purchased credit monitoring in an attempt to protect her credit, and safe guard her identity.

14. In addition to the monitoring her accounts for fraudulent activity affecting Ms. Torres as a result of the Breach, she will continue to be at heightened risk for financial fraud, medical fraud and identity theft and her attendant damages for years to come.

15. Defendant BHI is a not-for -profit, integrated health care system serving over 800,000 people throughout western New England. BHI's principal office is located at 759 Chestnut Street, Springfield, Hampden County, Massachusetts.

JURISTICTION AND VENUE

16. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million, exclusive of interest and costs. There are more than 100 putative class members, and at least some members of proposed Class have a different citizenship from BHI.

17. This Court has jurisdiction over Defendant as it operates in this District, and their computer systems implicated in this Breach are based in this District.

18. Plaintiff was a patient of BHI Health and engaged in underlying health services within this District where her PII was also maintained, and where the breach occurred which led to her sustaining damage. Through its business operations in this District, BHI intentionally avails itself of the markets within this District to render the exercise of jurisdiction by this Court just and proper.

19. Venue is proper in this Court pursuant to 28 U.S.C. § 1391 (a)(1) because a substantial part of the events and omissions giving rise to this action occurred in this District, BHI is based in this District, maintains patient PII in the District and has caused harm to Plaintiff and Class members residing in this District.

STATEMENTS OF FACTS

Background

20. Cyber-attacks come in may forms. Phishing attacks are among the oldest and well known. In simple terms, phishing is a method of obtaining personal information using deceptive emails and websites. The goal is to trick an e-mail recipient into believing that the message is something they want or need for a legitimate or trustworthy source and to subsequently click on link or download an attachment. The fake link will typically mimic a familiar website and require the input of credentials. Once input, the credentials are then used to gain unauthorized access into a system. "It's one of the oldest types of cyberattacks, dating back to the 1990's and one that every organization with an internet presence is aware."[2]

21. Phishing attacks are well known and understood by cyber-protection community and there are many well-known proactive measures that can be undertaken to prevent phishing attacks such as "sandboxing" inbound e-mail[3], inspecting and analyzing web traffic, pen-testing an organization to find weak spots, and employee education, among many others.[4]

22. Data breaches, including those perpetrated by phishing attacks, have become widespread. In 2016, the number of U.S. data breaches surpassed 1,000, a record high and a forty percent increase in the number of data breaches from the previous year.[5] In 2017, a new record high of 1,579 breaches were reported representing a 44.7 percent increase over 2016.[6]

---

[2] https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html. (Last visited April 10, 2019)

[3] An automated process whereby emails with attachments and links are segregated to an isolated test environment, a "sandbox," wherein a suspicious file or URL may be executed safely.

[4] https://www.csoonline.com/article/2117843/phishing/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent-it.html. (last visited April 10, 2019)

[5] Identify Theft Resource Center, *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout* (January 19, 2017), available at https://www.idtheftcenter.og/surveys-studys/ (last visited April 10, 2019).

[6] Identity Theft Resource Center, 2017 Annual Data Breach Year-End Review, available at https://www.idtheftcenter.org/2017-data-breaches/ (last visited April 10, 2019).

The BHI Data Breach

23. On February 7, 2019, Defendant discovered than an unauthorized third party gained access to BHI's patient information through the use of phishing emails sent to BHI employees. Due to BHI's inadequate protocols and procedures to prevent such attacks, unauthorized parties gained unfettered access to the PII/PHI of approximately 12,000 current and former patients.[7]

24. But not until or about April 8, 2019, did BHI publicly announced that its system had been compromised by unauthorized third parties. The announcement came two months after they first noticed their system had been compromised. BHI made no statement as to when the breach first occurred, or how long the privacy of patient PII had been compromised. A similar notice to the Plaintiff stated:

> BHI Health is committed to protecting the security and confidentiality of our patients' information. Regrettably, we are writing to inform you that an incident that involves some of your information. We are writing to explain the incident, measures we have taken, and some steps you can take in response.
>
> Between February 7 and March 7, 2019, BHI learned of unauthorized access to a limited number of employee email accounts during that same time frame due to a phishing incident. We immediately secured each account, began an investigation, and hired a leading computer forensic firm to assist. The investigation determined that one of the email accounts contained some information about you. The information may have included your name, address, date of birth, health insurance plan and policy information, and some limited health information, such as diagnosis, treatment, and/or procedure descriptions. The emails did not contain your Social Security number. Your electronic medical record was not accessed or involved.
>
> While we have no indication that your information was actually acquired or viewed by the unauthorized person, or that it has been misused, we wanted to notify you regarding this incident and assure you that we take it very seriously. As a precaution, we recommend that you review the statements you receive from your healthcare provider or your health insurer. If you see services that you did not receive, please contact the insurer or provider immediately.

[7] Baystate Health: Confidential Patient Info Accessed in Email Phishing Attach. April 8, 2019. https://www.nbcboston.com/news/local/Baystate-Health-Confidential-Patient-Info-Accessed-in-Phishing-Attack-508271191.html (last visited April 10, 2019).

> We deeply regret any inconvenience or concern that incident may cause you. To help prevent something like this from happening in the future, we required a password change for all affected employees, increased the level of email logging and are reviewing those logs regularly, and have blocked access to email accounts outside of our network unless the access is approved by BHI. We are also reinforcing employee training on how to detect and avoid phishing emails. If you have any questions, please call 1-833-231-3361, Monday through Friday, between 9 a.m. and 6:30 p.m. Eastern Time.

25. BHI has not advised as to why it waited months to advise patients that their information had been compromised as a result of the breach.

BHI's Inadequate Cyber-Security Practices

26. Prior to the Data Breach, BHI advised in the Notice of Privacy Practices posted on its website that it "WE ARE COMMITTED TO THE PRIVACY OF YOUR MEDICAL INFORMATION."[8]

27. BHI further acknowledged that it is "required by law to maintain the privacy and security of your protected health information ("PHI") and "Let you know promptly if a breach occurs that may have compromised the privacy or security of your information."[9]

28. BHI represented that it would abide by these obligations, but failed to live up to its own promises, as well as its duties and obligations required by law and industry standards.

29. Contrary to its promises, BHI's conduct has instead been a direct cause of the impermissible release, disclosure, compromise, and publication of Class Members' PII/PHI, as well as the ongoing harm to Plaintiff and other Class Members.

[8] Notice of Privacy Practices, available at https://www.baystatehealth.org/notice-of-privacy-practices content/uploads/2017/11/summary_notice_privacy_practices.pdf (last visited April 10, 2019).
[9] Notice of Privacy Practices, available at https://www.baystatehealth.org/notice-of-privacy-practices content/uploads/2017/11/summary_notice_privacy_practices.pdf (last visited April 10, 2019).

30. BHI could have prevented this Data Breach which was based on a long and well-known hacking technique known as phishing, for which there are numerous and effective countermeasures.

31. Generally, organizations can mount two primary defenses to phishing scams: employee education and technical security barriers.

32. Employee education is the process of adequately making employees aware of common phishing scams and implementing company-wide policies requiring unknown links, attachments or requests to be sequestered and checked for authenticity. Employee education and established protocols for use of log-in credentials is the easiest method to assist employees in properly identifying fraudulent emails and prevent unauthorized access to personal information.

33. Organizations like BHI can also greatly reduce the flow of phishing emails by implementing certain security measures governing email transmissions. For example, organizations can use a simple email validation system that allows domain owners to publish a list of IP addresses that are authorized to send email on their behalf to reduce the amount of spam and fraud by making it harder for malicious senders to disguise their identities. Organizations can also use email authentication protocols that block email streams which have not been properly authenticated.

34. Unfortunately, BHI failed to employ any of these defenses to the detriment of Plaintiff and thousands of Class Members. As evidenced by the success of the phishing hack, it is clear that BHI failed to ensure that its employees were adequately trained on even the most basic of cybersecurity protocols, including:

a. How to detect phishing emails and other scams including providing employees examples of these scams and guidance on how to verify if emails are legitimate;

b. Effective password management and encryption protocols for internal and external emails;

c. Avoid responding to emails that are suspicious or from unknown sources;

d. Locking, encrypting and limiting access to computers and files containing sensitive information; and

e. Implementing guidelines for maintaining sensitive data.

37 BHI's failures handed criminals patient PII/PHI and put Plaintiff and Class members of Class at serious, immediate and ongoing risk for identity theft and fraud.

38. The Data Breach was caused by BHI's failure to abide by best practices and industry standards concerning the security of its computer systems. BHI did not comply with security standards and allowed its patients' PII/PHI to be compromised by failing to implement security measures that could have prevented or mitigated the Data Breach.

39. BHI failed to ensure that all its personnel with access to patient records were made aware of this well-known and well-publicized type of scam.

40. In addition, upon information and belief, BHI failed to take reasonable steps to clearly, conspicuously, and timely inform Plaintiff and the other Class Members of the nature and extent of the Data Breach. By failing to provide adequate and timely notice, BHI prevented Plaintiff and Class Members from protecting themselves from the consequences of the Data Breach.

41. This is not BHI's first Data Breach, BHI has previously suffered a similar Data Breach in 2016 affecting 13,000 patients.

Value of Personally Identifiable Information

42. BHI was well-aware, or reasonably should have been aware, that the PII/PHI it collects is highly sensitive and of significant value to those who would use it for wrongful purposes.

43. The FTC defines identify theft as "a fraud committed or attempted using the identifying information or another person without authority."[10] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person."[11]

44. Personal identifying information is a valuable commodity to identify thieves once the information has been compromised. As the FTC recognizes, once identity thieves have personal information, "they can drain your bank account, run up your credit cards, open new utility accounts, or get medical treatment on your health insurance."[12]

45. Identity thieves can use personal information, such as that of Plaintiff and Class members, which BHI failed to keep secure, to perpetrate a variety of crimes that harm victims. For instance, identity thieves may commit various type of government fraud such as: immigration fraud; obtaining a driver's license or identification care in the victim's name but with another's picture; using the victim's information to obtain government benefits; or filing a fraudulent tax return using the victim's information to obtain a fraudulent refund.

[10] 17 C.F.R. §248.201 (2013).
[11] *Id.*
[12] Federal Trade Commission. *Warning Signs of Identity Theft*. Available at: https://www.consumer.ftc.gov/articles/0271-warnings-signs-identity-theft- (last visited April 10, 2019).

46. A "cyber black market" exists in which criminals openly post stolen social security numbers and other personal information on multiple underground Internet websites. Such data is valuable to identity thieve because they can use victims' personal data to pen new financial accounts, take out loans in another person's name and/or incur charges on existing accounts.

47. Professionals tasked with trying to stop fraud and other misuse know that PII/PHI has real monetary value in part because criminals continue their efforts to obtain this data.[13] In other words, if any additional breach of sensitive data did not have incremental value to criminals, one would expect to see a reduction in criminal efforts to obtain such additional data over time. However, just the opposite has occurred. According to the Identity Theft Resource Center, 2017 saw 1,579 data breaches, representing a 44.7 percent increase over the record high figures reported a year earlier.[14]

48. At all relevant times, BHI knew, or reasonably should have known, of the importance of safeguarding PII/PHI and of the foreseeable consequences that would occur if its data security system was breached, including, the significant costs that would be imposed on its patients as a result of a breach.

The Effects of Unauthorized Disclosure of PII/PHI

49. The ramifications of the BHI's failure to keep its patients' PII/PHI secure are long lasting and severe. Once PII/PHI is stolen, fraudulent use of that information and damage to victims may continue for years.

[13] *Data Breaches Rise as Cybercriminals Continue to Outwit IT, CIO Magazine*, https://www.cio.com/article/2686167/data-breach/data-breaches-rise-as-cybercriminals-continue-to-outwit-it.html. (last visited April 10, 2019).
[14] 2017 Annual data Breach Year-End Review, https://www.idtheftcenter.org/2017-data-breaches, (last visited April 10, 2019).

50. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration has warned that identity thieves can use an individual's Social Security number to apply for additional credit lines. Such fraud may go undetected until debt collection calls commence months, or even years, later.

51. Stolen Social Security numbers also make is possible for thieves to file fraudulent tax returns, file for unemployment benefits, or apply for a job using a false identity. Each of these fraudulent activities is difficult to detect. An individual may not know that his or her Social Security number was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

52. Moreover, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. Even then, a new Social Security number may not be effective, as "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[15]

53. Additionally, the information compromised in the Data Breach is significantly more valuable than the mere loss of credit card information typical of recent large retailer data breaches. The PII/PHI compromised in the BHI's Data Breach is difficult, if not impossible, to change (i.e. Social Security numbers, names, addresses, dates of birth and medical records).

[15] *Victims of Social Security Number Theft Find It's Hard to Bounce Back*. NPR, Brain Naylor, Feb. 9, 2015, available at http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millions-worrying-about-indentiy-theft (last visited April 10, 2019).

54. This data, as one would expect, demands a much higher price on the black market. Martin Walter, senior director of cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[16]

55. It is well known and the subject of many media reports that PII/PHI is highly coveted and a frequent target of hackers. This information is targeted not only for identity theft purposes, but also for committing healthcare fraud including obtaining medical services under another's insurance. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medial identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[17] Despite well publicized litigation and frequent public announcements of data breaches by medical and technology companies, Defendant opted to maintain an insufficient and inadequate system to protect the PHI and PII of Plaintiff and Class members.

56. Unfortunately, and as is alleged below, despite all of this publicly available knowledge or the continued compromises of PII and PHI in the hands of third parties, such as health companies, Defendant' approach at maintaining the privacy of the Plaintiff's and the Class Members' PII and PHI was lackadaisical, cavalier, reckless, or at the very least negligent.

Plaintiff and Class Members Suffered Damages

57. The PII/PHI belonging to Plaintiff and Class members is private and sensitive in nature and was left inadequately protected by BHI, BHI did not obtain Plaintiff's or Class

[16] *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, Tim Greene, February 6, 2015, *available at* http://www.itworld.com/article/2880960/anthem-hack-personal-data-stoeln-sells-for-10x-price-of-stolen-credit-card-numbers.html (last visited April 10, 2019).

[17] Elinor Mills, Study: Medical identity theft is costly for victims, available at https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims/ (last visited April 10, 2019.

members' consent to disclose their PII to any other person as required by applicable law and industry standard.

58. The Data Breach was a direct and proximate result of BHI's failure to: properly safeguard and protect Plaintiff's and Class members' PII/PHI from unauthorized access, use, and disclosure, as required by various state and federal regulations, industry practices, and the common law; BHI's failure to establish and implement appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of Plaintiff's and Class members' PII; and protect against reasonable foreseeable threats to the security or integrity of such information.

59. BHI had the resources necessary to prevent a breach, but neglected to adequately invest in data security, despite the growing number of well-publicized data breaches.

60. Had BHI remedied the deficiencies in its data security systems, adopted security measurers recommended by experts in the field, BHI would have prevented intrusion into its systems and, ultimately, the theft of PII/PHI belonging to its patients.

61. As a direct and proximate result of BHI's wrongful actions and inaction and the resulting Data Breach, Plaintiff and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from identity theft and identity fraud, requiring them to take the time which they otherwise would have dedicated to other life demands such as work and family in an effort to mitigate the actual and potential impact of the Data Breach on their lives including, *inter alia*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial accounts, closely reviewing and monitoring their credit reports and accounts for unauthorized activity, and filing police reports. T his time has been lost forever and cannot be recaptured.

62. The ramifications of Defendant' failure to keep Plaintiff's and Class Members' data secure and severe. As explained by the Federal Trade Commission:

> Medical identity theft happens w hen someone steals your personal information and uses it to commit health care fraud. Medical ID thieves may use your identity to get treatment—even surgery—or to bilk insurers by making fake claims. Repairing damage to your good name and credit record can be difficult enough, but medical ID theft can have other serious consequences. If a scammer gets treatment in your name, that person's health problems could become a part of your medical record. It could affect your ability to get medical care and insurance benefits, and could event affect decisions made by doctors treating you later on. The scammer's unpaid medical debts also could end up on your credit report.[18]

63. PII/PHI—like the type disclosed in the breach—is particularly valuable for cybercriminals. According to SecureWorks (a division of Dell Inc.), "[i]t's a well known truism within much of the healthcare data security community that an individual healthcare record is worth more on the black market ($50, on average) than a U.S.-based credit card and personal identity with social security number combined."[19] The reason is that thieves "[c]an use a healthcare record to submit false medical claims (and thus obtain free medical care), purchase prescription medication, or resell the record on the black market."[20]

64. Similarly, the FBI Cyber Division, in an April 8, 2014 Private Industry Notification, advised:

> Cyber criminals are selling [medical] information on the black market at a rate of $50 for each partial EHR, compared to $1 for a stolen social security number or credit card number. HER can then be sued to file fraudulent insurance claims, obtain prescription medication, and advance identity theft. HER theft is also more difficult to detect, taking almost twice as long as normal identity theft.[21]

---

[18] Federal Trade Commission, Medical ID Theft: Health Information for Older People, available at https://www.consumer.ftc.gov/articles/0326-medical-id-theft-health-information-older-people (last visited March 16, 2019).
[19] *What's the Market Value of a Healthcare Record*, Dell SecureWorks (December 13, 2012), https://www.secureworks.com/blog/general-market-value-of-a-healthcare-record (last visited April 10, 2019).
[20] *Id.*
[21] Federal Bureau of Investigation, FBI Cyber Division Private Industry Notification (April 8, 2014), https://info.publicintelligence.net/FBI-HealthCareCyberInstrusions.pdf (last visited April 10, 2019).

65. Once use of compromised non-financial PII/PHI is detected, the personal an economic consequence to the data breach victims can be overwhelming. As reported by CreditCards.com:

> The Ponemon Institute found that 36 percent of medical ID theft victims pay to resolve the issue, and their out-of-pocket costs average nearly $19,000. Event if you don't end up paying out of pocket, such usage can wreak havoc on both medical and credit records, and clearing that up is a time-consuming headache. That's because medical records are scattered. Unlike personal financial information, which is consolidated and protected by credit bureaus, bits of your medical records end up in every doctor's office and hospital you check into, every pharmacy that fills a prescription and every facility that processes payments for those transactions.[22]

66. Research by Ponemon confirms that medical identity theft is costly and complex to resolve, and therefore it is critical for healthcare providers to take additional steps to assist victims resolve the consequences of the theft and prevent future fraud. In a 2014 study, Ponemon found that sixty-five percent (65%) of victims of medical identity theft in the study had to pay an average of $13,500 to resolve the resultant crimes[23], and only ten percent (10%) of those in the study reported having achieved complete satisfaction in concluding the incident.

67. The average time spent by those respondents who successfully resolved their situation was more than 200 hours, working with their insurer or healthcare provider to make sure their personal medical credentials were secure and verifying the accuracy of their personal health information, medical invoices and claims, and electronic health records. Indeed, fifty-nine percent (59%) of the respondents reported that their information was used to obtain healthcare services or treatments, and fifty-six percent (56%) reported that their information was used to

[22] Cathleen McCarthy, CreditCards, *How to Spot and Prevent Medical Identity Theft* (August 19, 2014), http://www.creditcards.com/credit-card-news/spot-prevent-medical-identity-theft-1282.php (last visited April 10, 2019).
[23] Jaclyn Fitzgerald, Ponemon Institute Study reveals 21.7% Rise in medical Identity Theft, HC Pro (March 2, 2015), http://www.hcpro.com/HIM-313785-865/Ponemon-Institute-study-reveals-217-rise-in-medicalidentity-theft.html (last visited April 10, 2019).

obtain prescription pharmaceuticals or medical equipment. Forty-five percent (45%) of respondents said that the medical theft incident had a negative impact on their reputation, primarily because of embarrassment due to the disclosure of sensitive health conditions (89% of the respondents), thirty-five percent (35%) said the person committing the fraud depleted their insurance benefits resulting in denial of valid insurance complains, and third-one percent (31%) said they lost their health insurance entirely as a result of the medical identity theft. Twenty-nine percent (29%) of the respondents reported that they had to make out-of-pocket payments to their health plan or insurer to restore coverage. Additionally, the study found that almost one-half of medical identity theft victims lose their healthcare coverage as a result of the identity theft, almost one-third have their insurance premiums rise, and forty percent (40%) were never able to resolve their identity theft.

68. Notwithstanding the seriousness of the Data Breach, BHI has not offered to provide the Plaintiff with any assistance or meaningful compensation for the costs and burdens—current and future—associated with the exposure of her PII/PHI. BHI has offer some Class members Credit Monitoring.

69. Moreover, it is incorrect to assume that reimbursing an individual for financial loss due to fraud makes that individual whole again. On the contrary, after conducting a study, the U.S. Department of Justice's Bureau of Justice Statistics found that "among victims who had personal information used for fraudulent purposes, 29% spent a month or more resolving problems" and that "resolving the problems caused by identity theft [could] take more than a year for some victims."

70. To date, the BHI has offered patients nothing more than what any citizen is already entitled to under the law and is woefully inadequate in light of the nature of the Breach.[24]

> We recommend that affected patients review the statements they receive from their healthcare providers and healthcare insurer. If they see services they did not receive, please contact the insurer or provider immediately. For those patients whose Social Security numbers were included in the email accounts, we are offering a complimentary one year membership of credit monitoring and identity protection services.[25]

71. A free credit report and the ability to freeze their accounts is not only a right that every citizen enjoys, it is grossly inadequate to protect the Plaintiffs and Class members from the threats they fact resulting from the PII/PHI that was exposed. Moreover, although credit monitoring can help detect fraud after it has already occurred, it has very little value as a preventive measure and does nothing to prevent fraudulent tax filings. As noted by security expert Brian Krebs, "although [credit monitoring] services may alert you when someone opens or attempts to pen a new line of credit in your name, most will do little—if anything—to block that activity. My take: If you're being offered free monitoring, it probably can't hurt to sign up, but you shouldn't expect the service to stop identity thieves from ruining your credit."[26]

72. As a result of the BHI's failures to prevent the Data Breach, Plaintiffs and Class members have suffered and will continue to suffer damages. They have suffered or are at increased risk of suffering:

a. The compromise, publication, theft and/or unauthorized use of PHII/PHI;

[24] See, https://www.usa.gov/credit-reports ("You are entitled to a free credit report from each of the three credit reporting agencies (Equifax, Experian, and TransUnion) once every 12 months") (Last visited April 10, 2019).
[25] https://www.baystatehealth.org/phishing
[26] Brian Krebs, Are Credit Monitoring Services Worth It?, KREBS ON SECRUITY, (March 19, 2014), http://krebsonsecurity.com/2014/03/are-credit-monitoring-services-worth-it/ (last visited April 10, 2019).

b. Out-of-pocket costs associated with the prevention, detection, recovery and remediation from identity theft or fraud;

c. Lost opportunity costs and lost wages associated with efforts expended and the loss of productivity from addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest and recover from identity theft and fraud;

d. The continued risk to their PII/PHI, which remains in the possession of BHI and is subject to further breaches so long as BHI fails to undertake appropriate measures to protect the PII/PHI in their possession; and

e. Current and future costs in terms of time, effort and money that will be expended to prevent, detect, contest, remediate and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class members.

73. BHI continues to hold the PII/PHI of its patients, including Plaintiff and Class members. Particularly because BHI has demonstrated an inability to prevent a breach or stop it from continuing event after being detected, Plaintiff and Class members have an undeniable interest in ensuring that their PII/PHI is secure, remains secure, and is not subject to further theft.

CLASS ACTION ALLEGATIONS

74. Plaintiff seeks relief on behalf of herself and as representatives of all others who are similarly situated. Pursuant to Fed. R. Civ. P. Rule 23(a), (b)(2), (b)(3) and (c)(4), Plaintiff seeks certification of a Nationwide class defined as follows:

> All persons whose personally identifiable information and protected health information was compromised as a result of the Data Breach announced by BHI in February 2019 (the "Class").

75. Excluded from the Class are BHI and any of its affiliates, parents or subsidiaries; all persons who make a timely election to be excluded form the Class; government entities; and the judges to whom this case is assigned, their immediate families, and court staff.

76. Plaintiff hereby serves the right to amend or modify the class definitions with greater specificity or division after having had an opportunity to conduct discovery.

77. The proposed Class meets the criteria for certification under Rule 23(a), (b)(2), (b)(3) and (c)(4).

78. **Numerosity. Fed. R. Civ. P. 23(a)(1).** Consistent with Rule 23(a)(1), the members of the Class are so numerous and geographically dispersed that the joinder of all members is impractical. The Data Breach implicates at lease 12,000 current and former BHI patients. BHI has physical and email addresses for Class members who therefore may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, internet postings, and/or published notice.

79. **Commonality. Fed. R. Ci. P. 23(a)(2) and (b)(3).** Consistent with Rule 23(a)(2) and with 23(b)(3)'s predominance requirement, this action involves common questions of law and fact that predominate over any questions affecting individual Class members. The common questions include:

a. Whether BHI had a duty to protect patient PII/PHI;

b. Whether BHI knew or should have known of the susceptibility of its systems to a data breach;

c. Whether BHI's security measures to protect their systems were reasonable in light of HIPAA requirements, FTC data security recommendations, and best practices recommended by data security experts;

d. Whether BHI was negligent in failing to implement reasonably and adequate security procedures and practices;

e. Whether BHI's failure to implement adequate data security measurers allowed the breach of its data systems to occur;

f. Whether BHI's conduct, including its failure to act, resulted in or was the proximate cause of the breach of its systems, resulting in the unlawful exposure of the Plaintiff's and Class members' PII/PHI;

g. Whether Plaintiff and Class members were injured and suffered damages or other losses because of BHI's failure to reasonably protect its systems and data network; and,

h. Whether Plaintiff and Class members are entitled to relief.

80. **Typicality. Fed. R. Civ. P. 23(a)(3).** Consistent with Rule 23(a)(3), Plaintiff's claims are typical of those of other Class members. Plaintiff is a BHI patient whose PII/PHI was exposed in the Data Breach. Plaintiff's damages and injuries are akin to other Class members, and Plaintiff seeks relief consistent with the relief sought by the Class.

81. **Adequacy. Fed. R. Civ. P. 23(a)(4).** Consistent with Rule 23(a)(4), Plaintiff is an adequate representative of the Class because Plaintiff is a member of the Class she seeks to represent; is committed to pursuing this matter against BHI to obtain relief for the Class; and has no conflicts of interest with the Class. Moreover, Plaintiff's Counsel are competent and

experienced in litigating class actions, including privacy litigation of this kind. Plaintiff intends to vigorously prosecute this case and will fairly and adequately protect the Class's interests.

82. **Superiority. Fed. R. Civ. P. 23(b)(3).** Consistent with Rule 23(b)(3), a class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no usual difficulties are likely to be encountered in the management of this class action. The quintessential purpose of the class action mechanism is to permit litigation against wrongdoers event when damages to an individual plaintiff may not be sufficient to justify individual litigation. Here, the damages suffered by Plaintiff and the Class are relatively small compared to the burden and expense required to individually litigate their claims against BHI, and thus, individual litigation to redress BHI's wrongful conduct would be impracticable. Individual litigation by each Class member would also strain the court system. Individual litigation creates the potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economies of scale, and comprehensive supervision by a single court.

83. **Injunctive and Declaratory Relief.** Class certification is also appropriate under Rule 23(b)(2) and (c). Defendant, through their uniform conduct, acted or refused to act on grounds generally applicable to the Class as a whole, making injunctive and declaratory relief appropriate to the Class as a whole.

84. **Rule 23(c)(4).** Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether BHI owed a legal duty to Plaintiff and the Class to exercise due care in collecting, storing and safeguarding their PII/PHI;

b. Whether BHI breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, using, transmitting, and safeguarding their PII;

c. Whether BHI failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether BHI timely, adequately, and accurately informed Class members that their PII/PHI had been disclosed without authorization; and

e. Whether BHI failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information disclosed and compromised in the Data Breach.

85. Finally, all members of the proposed Classes are readily ascertainable. BHI has access to patient names and addresses affected by the Data Breach. Using this information, Class members can be identified and ascertained for the purposes of providing notices.

COUNT I
NEGLIGENCE

86. Plaintiffs restate and realleges paragraphs 1 through 85 above as if fully set forth herein.

87. BHI's Notice of Privacy Practices acknowledges BHI's duty to protect the PHII/PHI of its patents, which include Plaintiff and Class Members.

88. Plaintiff and the Class Members entrusted their PII/PHI to BHI with the understanding that the BHI would safeguard their information.

89. Defendant had full knowledge of the sensitivity of the PII/PHI and the types of harm that Plaintiff and Class Members could and would suffer if the PII were wrongfully disclosed.

90. Defendant had a duty to exercise reasonable care in safeguarding, securing and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining and testing the Defendant's security protocols to ensure that Plaintiff's and Class Members' information in its possession was adequately secured and protected and that employees tasked with maintaining such information were adequately training on cyber security measures regarding the security of student, parent guardian and employee personal information.

91. Plaintiff and the Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant know of or should have known of the inherent risks in collecting and storing the PII/PHI of Plaintiffs and the Class, the critical importance of providing adequate security of that PII/PHI, the current cyber scams being perpetrated on employers, and that it had inadequate employee training and education and IT security protocols in place to secure the PII/PHI of Plaintiff and the Class.

92. Defendant's own conduct created a foreseeable risk of harm to Plaintiff and Class members. Defendant' misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant' misconduct also included its decision not to comply with industry standards for the safekeeping and encrypted authorized disclosure of the PII/PHI of Plaintiff and Class Members.

93. Plaintiff and Class Members had no ability to protect their PII/PHI that was in BHI's possession.

94. Defendant was in a position to protect against the harm suffered by Plaintiff and Class Members as result of the Data Breach.

95. Defendant has a duty to have proper procedures in place to prevent the unauthorized dissemination Plaintiff and Class members' PII/PHI.

96. Defendant have admitted that Plaintiff's and Class Members' PII/Phi was wrongfully disclosed to unauthorized third persons as a result of the Data Breach.

97. Defendant, through their actions and/or omissions, unlawfully breached their duty to Plaintiff and Class members by failing to exercise reasonable care in protecting and safeguarding the Plaintiff's and Class members' PII/PHI while it was within the BHI's possession or control.

98. Defendant improperly and inadequately safeguarded Plaintiff's and Class members' PII in deviation of standard industry rules, regulations and practices at the time of the Data Breach.

99. Defendant, through their actions and/or omissions, unlawfully breached its duty to Plaintiff and Class members by failing to have appropriate procedures in place to detect and prevent dissemination of its patients' PII/PHI.

100. Defendant, through their actions and/or omissions, unlawfully breached its duty to adequately disclose to Plaintiff and Class members the existence, and scope of the Data Breach.

101. But for the Defendant' wrongful and negligent breach of duties owed to Plaintiff and Class members, Plaintiff's and Class members' PII/PHI would not have been compromised.

102. There is a temporal and close causal connection between Defendant's failure to implement security measures to protect the PII/PHI of current and former patients and the harm suffered or risk of imminent harm suffered by Plaintiff and the Class.

103. As a result of Defendant' negligence, Plaintiff and the Class members have suffered and will continue to suffer damages and injury including, but not limited to: out-of-pocket expenses associated with procuring robust identity protection and restoration services; increased risk of future identity theft and fraud, the costs associated therewith; time spent monitoring, addressing and correcting the current and future consequences of the Data Breach; and the necessity to engage legal counsel and incur attorneys' fees, costs and expenses.

COUNT II
BREACH OF CONTRACT

104. Plaintiffs restate and realleges paragraphs 1 through 103 above as if fully set forth herein.

105. As set forth above, Plaintiff and Class members received healthcare services from BHI.

106. As set forth above, the contract between Plaintiff and Class members and BHI was supported by consideration in many forms including the payment of monies for healthcare services.

107. Plaintiff and Class members performed pursuant to these contracts, and satisfied all conditions, obligations, and promises of the agreements.

108. Under the contracts, BHI were obligated, as outlined in the Privacy Practices, to maintain the confidentiality of Plaintiff and Class member's PHI and PII.

109. As a result of BHI's breach of contract, by failing to adequately secure Plaintiff and Class member's PHI and PII, Plaintiff and Class members did not receive the full benefit of the bargain, and instead received services that were less valuable than described in the contracts. Plaintiff and Class members, therefore, were damages in an amount at least equal to the difference in value between what was promised and what BHI ultimately provided.

110. Also, as a result of BHI's breach of contract, Plaintiff and Class members have suffered actual damages resulting from the theft of their PHI and PII, and remain at imminent risk of suffering additional breaches in the future.

COUNT III
BREACH OF IMPLIED CONTRACT

111. Plaintiff restates and reallege paragraphs 1 through 110 above as if fully set forth herein.

112. Plaintiff and Class members were required to provide their personal information, to BHI as a condition of becoming a patient at BHI.

113. Implicit in the enrollment documents between BHI and its patients was the obligation that the information provided to it would be maintained confidentially and securely.

114. Defendant has an implied duty of good faith to ensure that the PII/PHI of Plaintiff and Class members in its possession were only used for purposes relevant to their interactions as patients of BHI.

115. Defendant had an implied duty to reasonably safeguard and protect the PII/PHI of Plaintiff and Class members from unauthorized disclosure or uses.

116. Additionally, Defendant implicitly promised to retain this PII/PHI only under conditions that kept such information secure and confidential.

117. Plaintiff and Class members fully performed their obligations under the implied contracts with Defendant. Defendant did not.

118. Plaintiff and Class members would not have provided their confidential PII/PHI to the Defendant in the absence of their implied contracts with Defendant.

119. Defendant breached the implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff's and Class members' PII/PHI, which was compromised as a result of the Data Breach.

120. Defendant breached their implied contracts with Plaintiff and Class members by failing to reasonably safeguard and protect Plaintiff's and Class members' PII/PHI, which was compromised as a result of the Data Breach.

121. As a direct and proximate result of Defendant' breach of its implied contracts with Plaintiff and Class members, Plaintiff and Class members have suffered and will suffer injury, including but not limited to: (i) the loss of the opportunity how their PII/PHI is used; (ii) the compromise, publication, and/or theft of their PII/PHI; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII/PHI; (iv) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach; (vi) the continued risk to their PII/PHI, which remain in BHI's possession and is subject to further unauthorized disclosures so long as the BHI fails to undertake appropriate and adequate measures to protect the PII/PHI of Plaintiff and Class members in its continued possession; (vii) future costs in terms of time, effort and money that will be expended to prevent, detect, contest, and repair the impact of the PII/PHI compromised as a result of the Data Breach for the remainder of the lives of the Plaintiff and Class members; and (viii) the necessity to engage legal counsel and incur attorneys' fees, cost and expenses.

COUNT IV

NEGLIGENCE *PER SE*

122. Plaintiff restates and reallege paragraphs 1 through 85 above as if fully set forth herein.

123. Pursuant to HIPPA and the laws of numerous states, BHI had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' medical information.

124. BHI breached its duties to Plaintiffs and Class Members' under the aforementioned laws by allowing confidential medical information to be accessed and compromised by an unauthorized third party.

125. BHI's failure to comply with applicable laws and regulations constitutes negligence *per se*.

126. But for BHI's negligent breach of their duties, Plaintiff and Class Members would not have been injured.

127. The injury and harm suffered by the Plaintiff and Class Members was the reasonably foreseeable result of BHI's breach of its duties. BHI knew or should have known that it was failing to meet its duties, and that BHI's breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their confidential medical information.

128. As a direct and proximate result of BHI's negligent conduct and/or negligent supervision, Plaintiff and Class members have been injured and are entitles to damages.

COUNT V
INVASION OF PRIVACY

129. Plaintiff restates and reallege paragraphs 1 though 85 above as if fully set forth herein. Plaintiff and Class members had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

130. The unauthorized release to, custody of and examination by third parties of personal medical information and other personally identifiable information would be offensive to a reasonable person of ordinary sensibilities.

131. BHI owed a duty to its patients, including Plaintiff and Class Members, to keep their PII and PHI confidential.

132. The Data Breach at the hands of BHI constitutes an intentional interference with Plaintiff's and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

133. As a proximate result of the above acts and omissions of BHI, the PII and PHI of the Plaintiff and Class Members was disclosed to and used by third parties without authorization, causing Plaintiff and Class Members to suffer damages.

COUNT VI
DECLARATORY JUDGMENT

134. Plaintiff restates and realleges paragraphs 1 through 85 above as if fully set forth herein.

135. As previously alleged, BHI owes duties of care to Plaintiff and Class Members that require it to adequately secure such PII/PHI.

136. BHI still possesses Plaintiff's and Class members' PII/PHI.

137. In conjunction with alerting the public to the Data Breach, BHI represented that it: (a) secured the impacted accounts to prevent further unauthorized access; (b) confirmed the security of its email system; (3) notified law enforcement; and (4) retained a forensic security firm to investigate. The announcement lacked any specificity and, moreover, was wholly insufficient to ensure the PII/PHI still in BHI's possession is protected from further exposure.

138. Accordingly, BHI has not satisfied its contractual obligations and legal duties to Plaintiff and Class members. In fact, now that BHI's lax approach towards data security has become public, the PII in its possession is more vulnerable than before.

139. Actual harm has risen in the wake of the Data Breach regarding BHI's contractual obligations and duties of care to provide data security measures to Plaintiff and Class Members.

140. Plaintiff, therefore, seeks a declaration that (a) BHI's existing data security measures do not comply with its contractual obligations and duties of care, and (b) in order to comply with its contractual obligations and duties of care, BHI must implement and maintain reasonable security measures, including, but not limited to:

a. engaging third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on BHI's system on a periodic basis, and ordering BHI to promptly correct any problems or issues detected by such third-party security auditors;

b. engaging third-party security auditors and internal personnel to run automated security monitoring;

c. auditing, testing, and training its security personnel regarding any new or modified procedures;

d. segmenting customer data by, among other things, creating firewalls and access controls so that if one area of BHI is compromised, hackers cannot gain access to other portions of BHI systems;

e. purging, deleting, and destroying patient data not necessary for its provisions of services in a reasonably secure manner;

f. conducting regular database scans and security checks;

g. routinely and continually conducting internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

h. educating its patients about threats they face as a result of the loss of their personal information to third parties, as well as the steps BHI customers should take to protect themselves.

WHEREFORE, Plaintiff, on behalf of herself and all others similarly situated, respectfully requests the following relief:

i. An Order certifying this case as a class action;

j. An Order appointing Plaintiff as the class representative;

k. An Order appointing undersigned counsel as class counsel;

l. A mandatory injunction directing the Defendant to hereinafter adequately safeguard the PII/PHI of the Class by implementing improved security procedures and measures;

m. An award of damages;

n. An award of costs and expenses;

o. An award of attorneys' fees; and

p. Such other and further relief as this court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs demand a jury trial as to all issues triable by a jury.

Dated: April 11, 2019

Respectfully submitted,
The Plaintiff,
By her attorney,

Kevin Chrisanthopoulos, Esq.
KC Law
30 Court Street, Suite 1
Westfield, MA 01085
Tel. (413) 251-1010
Fax. (413) 372-1610
Kevin@KCTrialAttorney.com
BBO #643734